# Cell 分解による $p$ 進体の量化記号消去(体のモデル理論とその応用)

AUTHOR(S):

井深, 真悟

CITATION:

井深, 真悟. Cell 分解による $p$ 進体の量化記号消去(体のモデル理論とその応用). 数理解析研究所講究録 2006, 1515: 72-80

ISSUE DATE:

2006-09

URL:

http://hdl.handle.net/2433/58695

数理解析研究所講究録
1515巻 2006年 72-80



# Cell分解による$p$進体の量化記号消去

神戸大学大学院自然科学研究科　井深真悟 (Shingo Ibuka)
Kobe University Graduate School of Science and Technology

**$\mathcal{L}$-理論$T$が量化記号消去 (QE) を許す**とは，各$\mathcal{L}$-論理式$\varphi(\bar{x})$に対して，量化記号を持たない$\mathcal{L}$-論理式$\psi(\bar{x})$で，$T \models \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$を満たすものがあることである．

QEを許す理論のよく知られた例として，端点のない稠密な全順序集合，実閉（順序）体，代数閉体の公理などがあり，また整数の加法群や$p$進体の理論もある言語でQEを許す．

$p$進体のQEにはいくつかの方法が知られているが，本稿で紹介するのは，数論・数理論理学の研究者のJ.Denefによるセル分解によるアプローチ [10] である．

**歴史**

QEとセル分解についての歴史を簡単に振り返ってみたい．

実閉体と$p$進体のQE

| | |
|---|---|
| 1931年　「実数の定義可能集合について」(Tarski) | [1] |
| 1951年　実閉体のQE(Tarski) | [2] |
| 1975年　セル分解を用いた実閉体のQE(Collins) | [7] |
| 1965-66年 $p$進体のQE(Ax and Kochen) | [4] [5] |
| 1969年　実数体と$p$進体に決定手続きを与える (Cohen) | [6] |
| 1976年　$p$進体のQEがより自然な言語で示される (MacIntyre) | [8] |
| 1984年　QEによるポワンカレ級数の有理性証明 (Denef) | [9] |
| 1986年　セル分解を用いた$p$進体のQEを証明 (Denef) | [10] |

Tarskiは実閉体のQEを1951年に示しているが，既に彼は1931年の「実数の定義可能集合について」によって，ある形でQEを得ていたと言われている [11, p.85]．QEによって，実閉体の定義可能集合は「セル」と呼ばれる単純な集合の有限和に分解できる事が判るが，逆にセル分解を先に行うことでQEを示したのがCollins(1975)である．TarskiのQEは計算量上非現実的なものであったが，Collinsの方法はその高速さのためその後の実装の基軸となった．

$p$進体の場合もこれに似た流れがある．最初に$p$進体のQEを達成したのはAxとKochen(1965-66)である．しかし彼らの用いた言語はcross-sectionを含み，どの集合が定義可能なのか

が判別しにくいものであった．そこでMacIntyre(1976)はAx-KochenやErsov [3] の結果を用いて，より単純な言語において$\mathbf{Q_p}$のQEを行った．

この結果を数論に応用したのがDenef(1984)である．彼はMacIntyreのQEを利用して，$\mathbf{Z_p}$上の積分として与えられるある種のゼータ関数が有理関数である事を示した．この事実は特異点解消定理を用いた証明によって以前から知られていたが，Denefは積分領域をQEを用いてセル分解することで，変数分離・逐次積分を可能にし，別証明を与えた．

その後Denef(1986)自身が，逆にセル分解からQEを導いたのが[10]であり，本稿ではこの概略を述べる．なお著作中で彼はCohen(1969)のアイディアに基づいた方法であると繰り返し述べている．

### $p$進体 $\mathbf{Q_p}$

[10]では$\mathbf{Q_p}$の有限次拡大体においてのQEを行っている．以下では話を簡単にするために$\mathbf{Q_p}$に限るが，有限次拡大体でも同様にできる．

$x \in \mathbf{Q}^*(=\mathbf{Q}\setminus\{0\})$は次のように一意的に表せる．

$$x = p^n a/b \quad (\text{ただし } a,b,n \in \mathbf{Z},\ b>0,\ a,b,p \text{は互いに素})$$

このときの$n$を$ord(x)$と書き，$ord$を**$p$進付値**という．ただし$ord(0)=\infty$とする．**$p$進絶対値**$|\cdot| := p^{-ord(\cdot)}$で定まる距離に関して$\mathbf{Q}$を完備化して得られるのが**$p$進体 $\mathbf{Q_p}$**である．$\mathbf{Z_p}=\{x\in\mathbf{Q_p} \mid ord(x)\geq 0\}$の元を**$p$進整数**と呼ぶ．

$\mathbf{Q_p}$の構成法はいくつか知られているが，[10]は次のような**$p$進展開**を想定するとよい．$x\in\mathbf{Q_p^*}$は次のように一意に展開される．

$$x = a_r p^r + a_{r+1}p^{r+1} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots$$

ただし，$a_i \in \{0,1,\cdots,p-1\}$

逆に$p$進展開は$p$進数をひとつ定める．

$r=ord(x)$であるから，$x,y\in\mathbf{Q_p^*}$に対し以下の性質も明らかである．

$$ord(xy) = ord(x)+ord(y) \quad \cdots \quad (1)$$

$$ord(x)<ord(y) \text{ならば，} ord(x+y)=ord(x) \quad \cdots \quad (2)$$

$x\in\mathbf{Q_p^*}$の**angular component** $ac$を$ac(x)=p^{-ord(x)}x$で定める．これは，$p$進展開で考えたときの「仮数部」であり，「指数部」$ord(x)$と併せて$x=p^{ord(x)}ac(x)$と表すことができる．

### 言語

次のMacIntyreによる言語$\mathcal{L}_M$でQEを考えていく．

$$\mathcal{L}_M = \{+,-,\cdot,0,1\}\cup\{P_n \ :\ n\geq 2\}$$

ただし，$P_n(x)$は$(\exists y)x=y^n$（$n$乗根が存在する）と解釈する．なお体や付値体の言語ではQEは成功しない．(反例は[8, Appendix])

### べき剰余

$x\in\mathbf{Q_p^*}$の**$n$乗剰余**とは，次を満たす$z$のことである：$x=zy^n$となる$y\in\mathbf{Q_p^*}$がある．

$n$乗剰余のとり方は一意的ではないが，予め$n$で定まった有限集合から選べるようにできる．それは次のHensel-Rychlikの補題から判る．

**Hensel-Rychlik の補題**

$f(t) \in \mathbf{Z_p}[t]$, $\alpha \in \mathbf{Z_p}$, $e \in \mathbf{N}$

$|f(\alpha)| \leq p^{-(2e+1)}$, $p^{-e} \leq |f'(\alpha)|$ ならば

$f(\beta) = 0$ なる解 $\beta$ が $|\beta - \alpha| \leq p^{-(e+1)}$ にとれる.

ここで $f(t) = t^n - u$ とすると,

$\mathbf{Z_p} \ni u \equiv 1 \ mod \ p^{2ord(n)+1}$ ならば $u \in P_n$ $\cdots$ (3)

(3) を用いてべき剰余が有限通りしかないことが以下のようにわかる.

もし $x$ と $y$ が,

$ord(x) \equiv ord(y) \ mod \ n$ かつ,

$ac(x) \equiv ac(y) \ mod \ 2ord(n) + 1$

の関係にあれば, $ac(x/y)$ が (3) の仮定を満たし, $ac(x/y) \in P_n$. 従って $x/y = p^{kn} ac(x/y) \in P_n$, すなわち $x$ と $y$ は同じ $n$ 乗剰余を持つ. $x$ と $y$ は有限通りにしか分類されないから, べき剰余は有限である. □

なお [10] 本文には, このように $ord$ と $ac$ に着目し, べき剰余に還元することで有限通りに落としてしまう議論が頻繁に現われる.

**$\mathcal{L}_M$ の論理式**

QE のためには $\exists$ をひとつ消去すればよい. まず量化記号のない (**qf, quantifier-free**) 論理式を整理しておく. qf 論理式は次の形の論理式を $\bigvee$ と $\bigwedge$ で結合したものである:

$f \in P_n$, $f \notin P_n$, $f = 0$, $f \neq 0$ (ただし $f$ は $\mathbf{Q_p}$ 係数多項式)

ところが実際には最初のものしか必要ない. $=$ は以下のように $P_2$ に帰着できる.

$f = 0 \leftrightarrow (\exists z) pf^2 = z^2 \leftrightarrow pf^2 \in P_2$

(←:両辺の $ord$ を考えれば偶数でも奇数でも矛盾するので $ord$ は無限大.)

また, negation は次のように消去できる.

$f \notin P_n \leftrightarrow f$ の $n$ 乗剰余は 1 でない $\leftrightarrow \rho_1 f \in P_n \ \vee \cdots \vee \rho_m f \in P_n$

べき剰余が有限通りしかないから, 適当な $\rho_i \in \mathbf{Z_p}$ たちを用いて, 1 以外のべき剰余を全て書き出せばよい. 従って与えられた qf 論理式は次の形になる.

$\bigvee \bigwedge f_i \in P_{n_i}$

さらに $P_{n_i}$ も全体で共通にできる. $n$ を $n_i$ たちの公倍数とする. 一般に 2 つの元が同じ $n$ 乗剰余を持てば同じ $n_i$ 剰余を持つから, $n_i$ 剰余が 1 になるような $n$ 乗剰余をすべて挙げれば同値にできる:

$f \in P_{n_i} \leftrightarrow \rho_1 f \in P_n \vee \cdots \vee \rho_m f \in P_n$.

結局, $\mathcal{L}_M$ での QE は,

$\exists t \bigvee \bigwedge f_i(\bar{x}, t) \in P_n \leftrightarrow \bigvee \bigwedge g_j(\bar{x}) \in P_m$

なる消去を行うことである.

**Semi-algebraic 関数**

重要な概念のひとつが semi-algebraic 関数である. この関数のクラスは QE を用いると定義可能な関数のクラスに一致することが判る.

関数 $f$ が **semi-algebraic** であるとは,

$S$ が qf 定義可能なら, $\{(\bar{x}, \bar{y}) \mid (f(\bar{x}), \bar{y}) \in S\}$ も qf 定義可能

を満たすこととする．これは，qf論理式に現れる変項にその関数を代入した論理式も，あるqf論理式と同値になるということである．ゆえに，もし多項式 $f$ を用いて定義された集合がqf定義可能であれば，$f$ の仮定をsemi-algebraicに緩めてもqf定義可能である．例えば，$\{x \mid ord(f(x)) \geq 0\}$ は，(3)により $1+pf^2 \in P_2$ もしくは $1+pf^3 \in P_3$ で(qf)定義可能であるが，$s$ がsemi-algebraic関数ならば，

$$\{x \mid ord(s(x)) \geq 0\} = \{x \mid s(x) \in \{y \mid ord(y) \geq 0\}\} \qquad \cdots \quad (4)$$

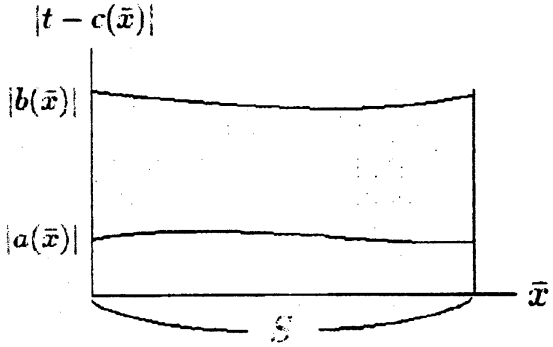
もqf定義可能になる．

semi-algebraic関数全体は多項式を含み，加減乗除と合成で閉じていることがすぐ判る．

**セル分解**

セル分解によって，多項式 $f_i$ たちのべき剰余を局所的に一定にし，さらにある種の変数分離を行うことができる．まずセルの定義をしよう．図では，縦軸方向は $p$ 進絶対値を用いて示してある．

**セル**とは，次のように表される集合である
$\{(\bar{x},t) \mid \bar{x} \in S,\ |a(\bar{x})| \leqq |t-c(\bar{x})| \leqq |b(\bar{x})|\}$
$S$：qf定義可能集合
$a(\bar{x}), b(\bar{x}), c(\bar{x})$：semi-algebraic関数
$c(\bar{x})$ を**セルの中心**という




ただし≦を，<に置き換えたり，条件を外したりしたものもセルとして認める．セルは(4)によりqf定義可能である．また図では稠密に見えるが，実際には $p$ 進距離を用いているので縦軸のとる値は離散的である．

セル分解定理はIとIIからなる．$\bar{x} \in \mathbf{Q_p}^m$ とする．

**セル分解定理 I**

$$f(\bar{x},t) = a_0(\bar{x}) + a_1(\bar{x})t + \cdots + a_k(\bar{x})t^k$$

（ただし，$a_i(\bar{x})$ は $x$ のsemi-algebraic関数）

ならば，$\mathbf{Q_p}^{m+1}$ を次を満たすような有限個のセルに分解できる．
各セルにおいて，中心 $c(\bar{x})$ を用いて

$$f(\bar{x},t) = b_0(\bar{x}) + b_1(\bar{x})(t-c(\bar{x})) + \cdots + b_k(\bar{x})(t-c(\bar{x}))^k$$

と表すと，$e>0$ が存在して，

$$|f(\bar{x},t)| \geq e|b_i(\bar{x})(t-c(\bar{x}))^i| \quad (0 \leq \forall i \leq k)$$

Iの意味するところは，多項式の絶対値は，ある項の絶対値の近くの有限通りの値しか取らないようにできるという事である．実際には，ほとんどの場合はある項の絶対値に一致する．

**セル分解定理 II**

Iと同様の多項式 $f_i(\bar{x},t)$ と $n \in \mathbf{N}$ に対して，

$\mathbf{Q_p}^{m+1}$ を次を満たすような有限個のセルに分解できる.
各セルにおいて, 中心 $c(\bar{x})$ を用いて

$$f_i(\bar{x},t) = b_0(\bar{x}) + b_1(\bar{x})(t-c(\bar{x})) + \cdots + b_k(\bar{x})(t-c(\bar{x}))^k$$

と表すと,

$$f_i(\bar{x},t) = u_i(\bar{x},t)^n b_i'(\bar{x})(t-c(\bar{x}))^{\nu_i}.$$

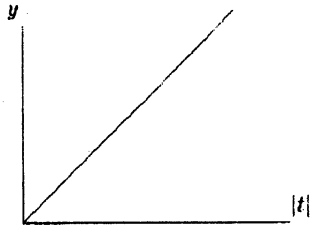
ここで, $|u_i(\bar{x},t)| = 1$, $b_i'(\bar{x})$ は semi-algebraic 関数, $\nu_i \in \mathbf{N}$.

IIは, 多項式 (の組) のべき剰余をセルの上で一定にできるというもので, QEの直接的な鍵である. 実際には, ほとんどの場合はある項のべき剰余に一致する.

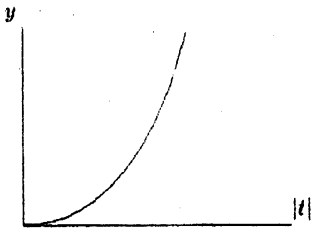
以下, 具体例を用いてセル分解定理Iの証明の様子を紹介する.

$$f(x,t) = t^p - x^{p-1}t$$

に対して, $\mathbf{Q_p^2}$ がどのようにセル分解されるのか見ていく.
まず $f$ のグラフを描く. $f$ の各項のグラフは (1) から次のようになる.




$y = |x^{p-1}t| = |x^{p-1}||t|$




$y = |t^p| = |t|^p$

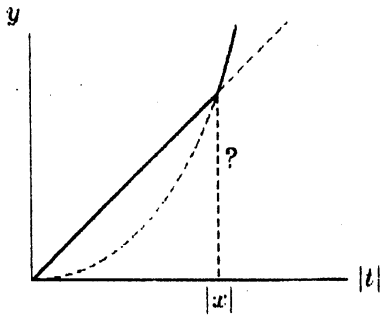
$x$ は固定して考えている. また $x$ 方向の分解も示さないが, ここでは特に問題にならない.
(2) により,

$$y = max\{|t^p|, |x^{p-1}t|\} \quad \underline{\text{if } |t^p| \neq |x^{p-1}t|}$$

であるから,

$$f(x,t) = |t^p - x^{p-1}t|$$

のグラフは, 各項のグラフの組み合わせで右図のようになる. ただし, $|t| = |x|$ のところでは, $|f(x,t)|$ は一意に定まらない.

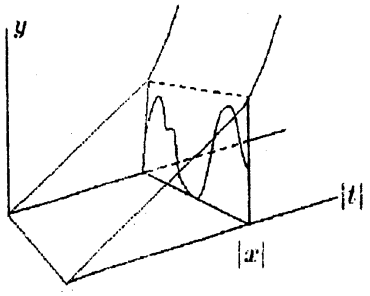



$f(x,t) = |t^p - x^{p-1}t|$

そこで少々強引に「次元」を増やすと右図のように描ける. ここで, 以下の3つにセル分解する.

$$|t| > |x|, \ |t| < |x|, \ |t| = |x|$$

前の2つのセルでは, セル分解定理Iの要求は満たされているのは明らかである. 3つめのセルをさらに分解する.



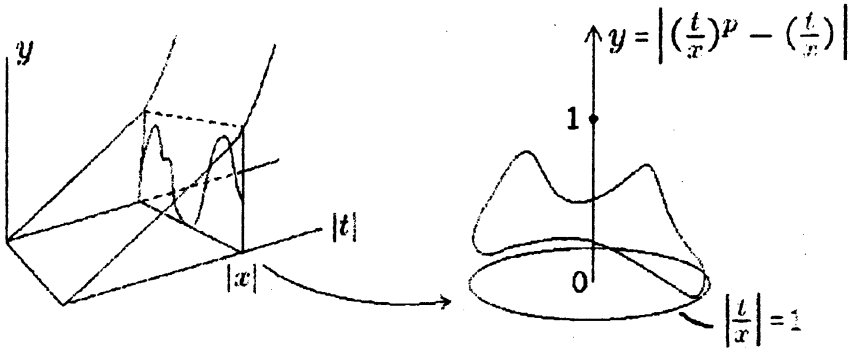

$f(x,t) = t^p - x^{p-1}t$

次のような変換を考える.

$$f(x,t) = t^p - x^{p-1}t \quad \text{on } |t| = |x|$$
$$\frac{f(x,t)}{x^p} = (\frac{t}{x})^p - (\frac{t}{x})$$

$u = t/x$ として,

$$g(x,u) = u^p - u \quad \text{on } |u| = 1$$




一般にこの変換はセル分解定理Iを保つようにできている：

$$\begin{aligned} & ord\ f(\bar{x},t) - \min_{i\geq 0} ord\ b_i(\bar{x})(t-c(\bar{x}))^i \\ = \quad & ord\ g(\bar{x},u) - \min_{i\geq 0} ord\ q_i(\bar{x})u^i \qquad \cdots \quad (5) \end{aligned}$$

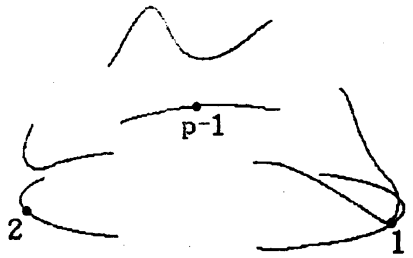
従って以後は，$f$ の代わりに $g$ に関するセル分解を行う.
この変換によって，$|u| = 1$ の形のセル上での，最大の絶対値を持つ係数が 1 であるような簡単な関数だけを扱えばよいことになる.

なお，セルの形を $|u| = 1$ にするために，semi-algebraic 関数全体がある性質を持つことが要請されている（「semi-algebraic 関数の導入」の章にて後述）.

ここで円周を $p-1$ 個にセル分解する.

$$|u-1| \leq \tfrac{1}{p}$$
$$|u-2| \leq \tfrac{1}{p}$$
$$\cdots$$
$$|u-(p-1)| \leq \tfrac{1}{p}$$

（中心がそれぞれ $1, 2, \cdots, p-1$ に変わる）




これは $u$ の $p$ 進展開における「1 の位」の場合分けであり，各円弧上では常に $\frac{1}{p} < |g| \leq 1$ か，常に $|g| \leq \frac{1}{p}$ となる．そこで $u = 1, 2, \cdots, p$ を代入して円弧を，

$$|g(x,u)| = |u^p - u| > \tfrac{1}{p}$$

なるグループとそれ以外に分類する.

$\frac{1}{p} < |g|$ を満たすセル上では，$|g|$ のとる値は有限通りであり，$|u| = |u^p| = 1$ なので，

$$|u^p - u| \geq e|u|, e|u^p| \quad \text{for some } e$$

が成り立つ．(5) から，

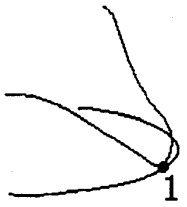
$$|f(x,t)| \geq e|t^p|, e|x^{p-1}t| \quad \text{on } |t - \kappa x| \leq |x|$$

となり分解定理Iの要求を満たしている.

一方，

$$|g(x,u)| = |u^p - u| \leqq \frac{1}{p}$$

のセルについては中心をとり直す．このグループのセルはその中に必ず $g$ の根を持つが，根を中心とした展開をとることで，$|g|$ をある項の絶対値に等しくできる．(実際には，この例の場合はとり直しをしなくてもよいが続けて手続きを見てみる)




根を持つことは Hensel-Rychlik の補題から判る：

$|g(\alpha)| \leq p^{-1}$，$p^0 \leq |g'(\alpha)|$ ならば，

$g(\beta) = 0$ なる解 $\beta$ が，$|\beta - \alpha| \leq p^{-1}$ にとれる．

例で扱っている $f$ に関しては，無条件で $|g'|$ に関する条件を満たす．

$$|g'(x,u)| = |pu^{p-1} - 1| = Max\{1/p, 1\} = 1$$

従って，このセルは $g$ の根を持つ．

なお，一般の場合 $|g'(\bar{x},u)|$ に関する条件は帰納法によって保証できる；$f'$ に関する分解を最初に得ておけば，

$$\begin{aligned} & ord\ f'(\bar{x},t) - \min_{i\geq 1} ord\ ib_i(\bar{x})(t-c(\bar{x}))^{i-1} \\ = \quad & ord\ g'(\bar{x},u) - \min_{i\geq 1} ord\ iq_i(\bar{x})u^{i-1} \qquad \cdots \quad (6) \end{aligned}$$

によって分解定理 I は $g'$ でも成立する．変換によって，$g$ の展開に現れる項の最大の絶対値は 1 であるから，$g'$ の展開項の絶対値もセル上で正の下限を持つ．(2) から $|g'|$ も正の下限を持つので，その値を参照して円周を分割すればよい．

セル分解定理 I の statement と変換は，(5) や (6) が成り立つように巧妙に用意してある．

さて，$g(x,u) = u^p - u$ の根 1 をセルの中心に採用し，展開しなおす．

$$g(x,u) = (u-1)^p +_p C_1(u-1)^{p-1} +_p C_2(u-1)^{p-2} + \cdots + 1(u-1).$$

| 各係数 | $\leqq 1$ と，$|u-1| \leqq 1/p$ を考えれば，

$$|g(x,u)| = |u-1|$$

でありこれでセル分解 I は完了した．

なお，$x$ を固定して考えているので表面化しないが，根でとりなおした「中心」は確かに $x$ の semi-algebraic 関数になる．

一般のセル分解定理 I は $f$ の次数に関する帰納法によって示されるが，そのとき平行してセル分解定理 II と，semi-algebraic 関数の持つ性質（「根でとった中心が semi-algebraic 関数で与えられる」を含む）の証明も同時に行う．

セル分解定理 II の証明は I に似ている．概要だけ述べる．関数 $f$ が一つの場合を考える．複数の場合は，それぞれに対してセル分解を行っておき，それらの intersection がまたセルと見なせる（ように中心が選べる）ことを示せばよい．

まず，帰納法の仮定によって $f$ に対するセル分解 I を行っておく．(3) を用いると，$\mathbf{Q_p}^{m+1}$ の殆どの部分で $f$ のべき剰余はひとつの展開項で決まる事が判る．この部分では II を満足する分解がとれている．そうでない場合は I と同じ変換で，有限個の簡単なセルと関数に帰着できる．予めとっておいた I の分解により，変換後の関数 $g(\bar{x},u)$ がセル上で有限通

りの絶対値しか持たないことが判る．この際，$f$ のべき剰余が一定になるようにさらに分解をするのはたやすい．

**QE**

$\varphi(\bar{x},t)$ を qf 論理式とする．セル分解定理 II により，QE の際には $\varphi$ は次の disjunction だと仮定してよい．

$$ord\ a_1(\bar{x}) \leq ord(t-c(\bar{x})) \leq ord\ a_2(\bar{x})$$
$$\bar{x} \in C \quad (\text{ただし } C \text{ は qf 定義可能集合})$$
$$b_i(\bar{x})(t-c(\bar{x}))^{\nu_i} \in P_n$$

上の 2 つがセルによる場合分けを表現している．3 つめは，$b_i$ と $t-c(\bar{x})$ のべき剰余によって $b_i(\bar{x})(t-c(\bar{x}))^{\nu_i}$ のべき剰余も決まることに注意すると，代わりに，

$$\rho(t-c(\bar{x})) \in P_n$$

の形を考えればよい．従って，$\exists t\varphi(\bar{x},t)$ は，

$$\exists l \in \mathbf{Z}\ (ord\ a_1(\bar{x}) \leq l \leq ord\ a_2(\bar{x}),\ l \equiv ord\ \rho^{-1}\ mod\ n)$$

と同値になる．(セルが縦線集合として定義してあるのは，このためであると思われる．)

$\gamma = ord\ a_1\rho\ mod\ n$ に応じてさらに次と同値になる．

$$ord(a_1(\bar{x})\rho) \leq\ ord(a_2(\bar{x})\rho) \qquad (\text{if } \gamma = 0)$$
$$ord(a_1(\bar{x})\rho) + n - \gamma \leq ord(a_2(\bar{x})\rho) \qquad (\text{if } \gamma \neq 0)$$

これらは (4) により qf 論理式で表現することができるし，$\gamma = 0, \cdots, n-1$ も qf 定義可能なので，これで QE が完了した．

**semi-algebraic 関数の導入について**

QE のためには，セル分解は多項式に対してだけ用意すればよいはずである．しかし実際には，多項式であるのはひとつの変数 $t$ に関してだけであって，係数に許される関数のクラス $\mathcal{F}$ は semi-algebraic まで広くとってある．その理由は以下によると思われる．

まず帰納法の都合上，$t$ に関する次数を小さくする必要があり，これを除算によって実現している．その分，$\mathcal{F}$ が除算で閉じている必要があった．

またセル分解定理の証明の中でセルを $|u|=1$ なる形に変換したが，これを行うためには $\mathcal{F}$ は次の操作でも閉じていなくてはならない：

$$\theta \in \mathcal{F},\ \frac{ord\ \theta}{n} \in \mathbf{Z} \text{ なら，} ord\ \eta = \frac{ord\ \theta}{n} \text{ となる } \eta \in \mathcal{F} \text{ がある} \qquad (n \in \mathbf{N}) \quad \cdots \quad (7)$$

これらの要件を満たすクラスとして，まず (qf) 定義可能関数全体が考えられるが，これを直接 $\mathcal{F}$ に採用することはできない．QE のためにはセルが定義から明らかに qf 定義可能である必要があり，$ord\ f \geq 0$ が qf 論理式で記述できなくてはならない．ところが一般の qf 定義可能関数 $f$ に対しては，$ord\ f \geq 0$ を qf 論理式で表現するのは QE そのものと同じくらい難しいからである．

一方，$ord\ x \geq 0$ は qf 論理式でかけるので，そこから $ord\ f(\bar{x}) \geq 0$ も qf 論理式で定義できることを直接要請しているのが semi-algebraic 関数である．

QE を事前に知っているから semi-algebraic という形で (qf) 定義可能関数を $\mathcal{F}$ に採用することができるのであるが，しかし，semi-algebraic 関数全体が (7) を満たすことを示すのはやはり難しく，セル分解と平行して証明する結果になっている．

# 参考文献

[1] Sur les ensembles definissables de nombres reels. I. Fundamenta Math., 17(1931), 210-39 (Trans. Logic, semantics, metamathematics Papers from 1923 to 1938, Oxford Clarendon Press(1956), 110-42)

[2] A.Tarski, A Decision Method for Elementary Algebra and Geometry, second ed., rev., Univ. of California Press, Berkeley, 1951.

[3] J. Ersov, On the elementary theory of maximal normed fields, Dokl. Akad. Nauk SSSR 165 (1965), 21-23.

[4] J. Ax and S. Kochen, Diophantine problems over local fields I, II, Amer. Journ. Math. 87 (1965), 605-630, 631-648

[5] J. Ax and S. Kochen, Diophantine problems over local fields, III: Decidable fields, Ann. of Math. (2) 83 (1966), 437-456.

[6] P.J.Cohen, Decision procedures for real and p-adic fields, Comm. Pure Appl. Math. 22(1969), 131-151

[7] G. E. Collins, Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition, In Lecture Notes In Computer Science, volume Vol. 33, 134-183. Springer-Verlag, Berlin, 1975.

[8] A.MacIntyre, On definable subsets of p-adic fields, J. Symb. Logic 41(1976), 605-610

[9] J.Denef, The rationality of the Poincare series associated to the p-adic points on a variety, Invent. Math. 77,1-23(1984)

[10] J.Denef, p-adic semi-algebraic sets and cell decomposition, J.reine angew. Math. 369(1986),154-166

[11] W.Hodges, Model Theory, Encyclopedia of mathematics and its applications, Cambridge university Press, 1993